IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Richmond Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	CRIMINAL NO. 3:19-CR-130-MHL
	)	
OKELLO T. CHATRIE,	)	
	)	
Defendant.	)	

UNITED STATES' RESPONSE TO AMICUS CURIAE BRIEF OF GOOGLE LLC

The United States of America, by its undersigned attorneys, submits this response to the Amicus Curiae Brief of Google LLC. (ECF No. 59-1.)

ARGUMENT

I. THE DEFENDANT VOLUNTARILY CONVEYED HIS LOCATION INFORMATION TO GOOGLE.

Google confirms that the defendant voluntarily conveyed his location information to Google, even under the demanding standard for voluntary disclosure used by the Supreme Court in *Carpenter v. United States*, 138 S. Ct. 2206 (2018). *Carpenter* held that cell-site information was not voluntarily conveyed to the phone company because it was collected "without any affirmative act on the part of the user beyond powering up," because there was "no way to avoid leaving behind a trail of location data," and because carrying a cell phone was "indispensable to participation in modern society." *Id.* at 2220. Google's description of how its location services function demonstrates that these factors do not apply to the Location History information obtained by investigators here.

First, Google details the multiple steps the defendant was required to take for Google to collect and store his Location History information:

> [Location History] functions and saves a record of the user's travels only when the user opts into [Location History] as a setting on her Google account, enables the "Location Reporting" feature for at least one mobile device, enables the device-location setting on that mobile device, permits that device to share location data with Google, powers on and signs into her Google account on that device, and then travels with it.

ECF No. 59-1 at 8. Thus, Google's storage of the defendant's location information took far more than him powering up his cell phone: he had to affirmatively opt in multiple times to enable Google's collection and storage of his Location History information.

Second, Google confirms that even after the defendant chose to have Google store his location information, he retained the ability to delete it: "[t]he user can review, edit, or delete her Timeline and [Location History] information from Google's servers at will." ECF No. 59-1 at 8. Thus, the defendant could have avoided having Google store his location information, unlike the cell-site information in *Carpenter*.

Third, Google's description of its location services makes clear that having Google store Location History information is not indispensable to participation in modern society. As an initial matter, Google states that "many of Google's products and services can be used without a Google account." ECF No. 59-1 at 5. Google Search is quite useful, but one need not have a Google account to use Google Search. In contrast, the benefits Google describes from enabling Location History seem minimal. According to Google, these benefits for an account holder include the ability to "obtain personalized maps or recommendations based on places she has visited, get help finding her phone, and receive real-time traffic updates about her commute," as well as "the ability to track one's own movements and enrich one's electronic footprint." ECF No. 59-1 at 6-7, 22. Access to such features is far from indispensable.

In sum, the defendant voluntarily disclosed his Location History information to Google because he opted in to its collection and storage, because he had the ability to edit and delete it, and because its collection and storage by Google is not indispensable to participation in modern society. Google is correct when it states that the defendant "errs in asserting that '[i]ndividuals do not voluntarily share their location information with Google.'" ECF No. 59-1 at 9.

II. THE DEFENDANT HAD NO REASONABLE EXPECTATION OF PRIVACY IN TWO HOURS OF GOOGLE LOCATION HISTORY INFORMATION.

The Supreme Court "has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *United States v. Miller*, 425 U.S. 435, 443 (1976). This principle did not control in *Carpenter* because the Court concluded that cell-site information "is not truly 'shared' as one normally understands the term." *Carpenter*, 138 S. Ct. at 2220. In addition, *Carpenter* held only that "accessing seven days of [cell-site information] constitutes a Fourth Amendment search." *Id.* at 2217 n.3. Here, the defendant voluntarily conveyed his location information to Google under the reasoning of *Carpenter*, and investigators obtained only two hours of that information, rather than a "comprehensive chronicle of the user's past movements." *Id.* at 2212. Google's disclosure of location information therefore was not a Fourth Amendment search.

Google's arguments that disclosure of two hours of the defendant's location information was a Fourth Amendment search lack merit. Google points out that Location History information is more precise than cell-site information, and it argues that Location History information therefore

implicates greater privacy interests than cell-site information. *See* ECF No. 59-1 at 10, 20. But as the United States explained in its Response Brief, the Supreme Court in *Carpenter* assumed that cell phone location information would approach the precision of GPS, so the greater accuracy of Google location information provides no basis for giving it enhanced Fourth Amendment protection. *See Carpenter*, 138 S. Ct. at 2218-19; ECF No. 21 at 8-9. In *Carpenter*, the Supreme Court found that a cell phone user had a reasonable expectation of privacy in "the whole of his physical movements." *Carpenter*, 138 S. Ct. at 2219. A two-hour interval of location information cannot meet this standard, regardless of the accuracy of individual points within the interval.

Google also argues that a warrant should be required for Location History information because when Google responds to a GeoFence warrant, it must "search across all Google users for their [Location History] information." ECF No. 59-1 at 23. Similarly, it notes that a GeoFence warrant "is not tied to any known person, user, or account." *Id.* at 11. These facts, however, do not distinguish GeoFence warrants from other forms of legal process that do not involve Fourth Amendment searches or require a warrant. For example, tower dumps are not tied to any known person, user, or account, but a tower dump is not a Fourth Amendment search. *See United States v. Adkinson*, 916 F.3d 605, 611 (7th Cir. 2019).

Moreover, service providers commonly review large sets of customer records to produce information in response to appropriately limited legal process. For example, in the traditional telephone context, investigators use subpoenas to identify the people who placed calls to a specified telephone number. Obtaining this information is not a search under *Smith v. Maryland*, 442 U.S. 735, 742-44 (1979), which held that telephone users voluntarily convey dialed phone number information to the phone company. A phone company responding to this sort of subpoena, however, may review call records for all of its customers to find this information. *See Ameritech*

Corp. v. McCann, 403 F.3d 908, 910 (7th Cir. 2005).

Similarly, the United States often uses a "specific and articulable facts" court order issued pursuant to 18 U.S.C. § 2703(d) to compel Google to disclose identity information for subscribers who accessed their Google accounts from a specified IP address during a particular time period. Internet users have no reasonable expectation of privacy in their IP address, *see United States v. Wellbeloved-Stone*, 777 F. App'x 605, 607 (4th Cir. June 13, 2019), so use of this investigative technique is not a search. Responding to such a court order, however, requires Google to review access records for all of its account holders. These examples demonstrate that a service provider's response to appropriately limited legal process does not become a search merely because the service provider must review a large set of records to find the responsive information.[1]

Google further asserts that the defendant retains a reasonable expectation of privacy in Google Location History information because it "is not compiled 'for . . . business purposes.'" ECF No. 59-1 at 22. As an initial matter, however, Google's Brief does not actually claim that Google does not use customer location information for its business purposes. Google states that location information is stored "primarily" for the user's benefit, ECF No. 59-1 at 8, but that formulation suggests that customer location information is also used for Google's business purposes. Google should clarify the extent to which it uses and benefits from customer location information, including both Location History information and any other Google databases that

[1] It would also be possible for Google to create an additional database of Location History information that would obviate its need to review the Location History information of all customers in response to a GeoFence warrant. Google could create a database that indexed Location History information based on its location in some sort of cellular grid. When Google received a GeoFence warrant, it would then need to review only location data from the relevant cell or cells, much like a tower dump. This possibility provides further evidence that producing GeoFence information does not become a search merely because Google reviews a large set of customer records: whether Google's production of GeoFence information constitutes a search for Fourth Amendment purposes should not depend on the internal structure of Google databases.

store location information pertaining to account holders.[2]

Moreover, even Google's limited discussion of its use of account holder location information shows that Google does in fact use that information for a "business purpose." Google compares location information to email, *see* ECF 59-1 at 22, but when an email service provider sends, receives, and stores email, it need not review or use the contents of the email. In contrast, Google's use and analysis of customer location information is essential to the location services it provides. For example, Google acknowledges that it uses account holder location information to provide "real-time traffic updates." ECF 59-1 at 7. This service requires Google to analyze location information sent to it by its customers and share the results of its analysis with other nearby customers. When a business uses information supplied by a customer to provide services, the customer retains no reasonable expectation of privacy in that information. For example, an individual retains no reasonable expectation of privacy in personal financial records shared with an accountant. *See Couch v. United States*, 409 U.S. 322, 335-36 (1973).

In addition, the principle that one retains no reasonable expectation of privacy in information revealed to a third party has never been limited to business records. For example, this principle applies to incriminating statements made in the presence of an informant. *See Hoffa v. United States*, 385 U.S. 293, 413-14 (1966). More generally, the roots of the third-party doctrine long predate *United States v. Miller* and *Smith v. Maryland*. It is an "ancient proposition of law" that the public "has a right to every man's evidence." *United States v. Nixon*, 418 U.S. 683, 709 (1974). The Supreme Court has recognized that "as early as 1612, . . . Lord Bacon is reported to have declared that 'all subjects, without distinction of degrees, owe to the King tribute and service,

[2] Google states that "[Location History] information was the only location information produced to the government in response to this geofence warrant," but it does not address whether it stores other databases containing location information. ECF No. 59-1 at 9.

not only of their deed and hand, but of their knowledge and discovery.'" *Blair v. United States*, 250 U.S. 273, 279-280 (1919) (quoting *Countess of Shrewsbury Case*, 2 How. St. Tr. 769, 778 (1612)). In this case, Google's role is fundamentally that of a witness: Google observed the location of people present at the robbery, and the government called upon it to disclose its observations. Allowing litigants to obtain information from witnesses is critical to the truth-seeking function of the justice system: "[t]he need to develop all relevant facts in the adversary system is both fundamental and comprehensive. The ends of criminal justice would be defeated if judgments were to be founded on a partial or speculative presentation of the facts." *Nixon*, 418 U.S. at 709. It was not a search when Google revealed its observations to investigators.

III. THIS COURT NEED NOT ADDRESS GOOGLE'S INTERPRETATION OF THE STORED COMMUNICATIONS ACT.

This Court need not consider Google's argument that as a statutory matter, the Stored Communications Act ("SCA") requires a warrant to compel Google to disclose location information. *See* 18 U.S.C. §§ 2701-13; ECF No. 59-1 at 14-18. Investigators in this case obtained a warrant for the defendant's location information, and his motion to suppress is based solely on his allegation of a Fourth Amendment violation, not a statutory violation. If the United States ever attempted to compel Google to disclose GeoFence information via a "specific and articulable facts" court order issued pursuant to 18 U.S.C. § 2703(d), Google would then have the opportunity to challenge that order.

Another reason why this Court need not consider the SCA here is because the SCA provides no suppression remedy for a statutory violation. The SCA includes criminal penalties and civil damages for certain types of violations of the SCA, *see* 18 U.S.C. §§ 2701 & 2707, and it further specifies that "the remedies and sanctions described in this chapter are the only judicial

remedies and sanctions for nonconstitutional violations of this chapter." 18 U.S.C. § 2708. Courts have thus held that statutory violations of the SCA do not result in suppression. *See United States v. Guerrero*, 768 F.3d 351, 358 (5th Cir. 2014) ("suppression is not a remedy for a violation of the [SCA]"); *United States v. Smith*, 155 F.3d 1051, 1056 (9th Cir. 1998) ("the [SCA] expressly rules out exclusion as a remedy"). Thus, even if the defendant were to allege a violation of the SCA here, the appropriate focus for this Court would still be the defendant's Fourth Amendment argument.

The United States notes, however, that there is some reason to doubt Google's analysis of how the SCA applies to Google location information. For one example, Google argues that under the SCA, Google location information "qualifies as 'contents' of 'electronic communications.'" ECF No. 59-1 at 16. But Google selectively quotes only a portion of the definition of "electronic communication." Google states: "The SCA defines an 'electronic communication' as a 'transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part' by an electronic system.'" *Id.* (quoting 18 U.S.C. § 2510(12)). Google ignores a potentially significant exclusion from this definition: the definition excludes "any communication from a tracking device (as defined in section 3117 of this title)." 18 U.S.C. § 2510(12)(C). Google elsewhere states that Google's location services give one "the ability to track one's own movements," which suggests that a user who opts in to Google Location History may be using a tracking device. *See* 18 U.S.C. § 3117 (defining a "tracking device" to mean "an electronic or mechanical device which permits the tracking of the movement of a person or object"). If the location information users send to Google is a communication from a tracking device, the location information could not be the contents of an electronic communication. Again, however, because interpreting the SCA is not necessary to resolve the defendant's suppression motion, this Court

should not address the SCA here.

CONCLUSION

Google confirms that the defendant voluntarily conveyed his location information to Google. This Court should deny the defendant's motion to suppress the fruits of the GeoFence warrant.

Respectfully submitted,

G. ZACHARY TERWILLIGER
United States Attorney

By: /s/

Kenneth R. Simon, Jr.
Peter S. Duffey
Assistant United States Attorneys
Eastern District of Virginia
919 E. Main Street, Suite 1900
Richmond, VA 23219
(804) 819-5400
Fax: (804) 771-2316
Email: Kenneth.Simon2@usdoj.gov

Nathan Judish
Senior Counsel, Computer Crime and
Intellectual Property Section
Criminal Division
United States Department of Justice

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 10th day of January, 2020, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which will send an electronic notification of such filing to the following:

Laura Koeing
Office of the Federal Public Defender (Richmond)
701 E Broad Street
Suite 3600
Richmond, VA 23219
Email: Laura_Koenig@fd.org

Paul Geoffrey Gill
Office of the Federal Public Defender (Richmond)
701 E Broad Street
Suite 3600
Richmond, VA 23219
Email: paul_gill@fd.org

Michael William Price
National Association of Criminal Defense Lawyers
1660 L Street NW
12th Floor
Washington, DC 20036
(202) 465-7615
Email: mprice@nacdl.org
PRO HAC VICE

_____/s/_____
Kenneth R. Simon, Jr.
Assistant United States Attorneys
Eastern District of Virginia
919 E. Main Street, Suite 1900
Richmond, VA 23219
(804) 819-5400
Fax: (804) 771-2316
Email: Kenneth.Simon2@usdoj.gov